The Official Action objected to the application for not including an abstract.   Responsively, an Abstract of the Disclosure is attached.

The specification has been amended to add section headings.

There are no other formal matters outstanding.

Claims 1 and 4 were rejected under §102(e) as being anticipated by GREEN et al. 6,003,084.

Claims 2 and 5 were rejected under §103(a) as being unpatentable over GREEN et al. in view of AZUMA et al. 6,430,150.

Claims 3 and 8 were rejected under §103(a) as being unpatentable over GREEN et al. in view of ENGEL 5,124,984.

Claim 6 was rejected under §103(a) as being unpatentable over GREEN et al. in view of BOEBERT et al. 5,864,683 and ENGEL.

Claim 6 was rejected under §103(a) as being unpatentable over GREEN et al. in view of BOEBERT et al.

Claim 9 was rejected under §103(a) as being unpatentable over GREEN et al. in view of BARR 4,763,357.

As amended, the independent claims are believed to be patentable over the applied references.   Accordingly, reconsideration and allowance of the independent claims and the claims depending therefrom are respectfully requested.

The GREEN et al. patent relates to a secure network proxy for connecting entities.   From GREEN et al., it is clear to

one of skill in the art that this reference concerns TCP/IP networks. Also, one of skill in the art would appreciate that GREEN et al. teach software provisions in the OSI model layers 4-7, and do not actually physically disconnect the communicating entities. Moreover, this would be clear to one of skill in the art as physical disconnection of the communicating entities is not possible at all in a TCP/IP network. This is because that in such a case, the complete network would fail, leading to the situation in which no communication is possible at all.

In GREEN et al., there is further no motivation for one of skill in the art that would lead him to apply the teachings of GREEN et al. to direct communication links, as per the recitations of amended independent claims 1 and 4. In any event, applicant believes it is clear that GREEN et al. neither teach nor suggest the communication link being physically interrupted. Accordingly, GREEN et al. can be neither anticipatory nor rendered obvious the pending independent claims.

In review, the present invention specifically tests the communication on the protocol used, i.e., it checks the protocol based on the electrical characteristics present in the communication link. When a non-standard (that is, an illegal) protocol is used, the communication link is completely interrupted. As recited in the amended claims, the link is physically interrupted between the first communication station and the second communication station. This provides excellent

6

protection against attempts from the outside to manipulate communication devices, e.g., by activating some hidden remote diagnostic system functionality, as described in the description of the present application.

In view of the applied reference neither teaching nor suggesting the recited features of the presently-pending independent claims, it is respectfully requested that these claims be allowed. As the dependent claims include all of the recitations of the independent claims from which they depend, the dependent claims are also believed to be allowable.

In view of the above, applicant believes that the present application is in condition for allowance and an early indication of the same is respectfully requested.

Attached hereto is a marked-up version of the changes made to the claims. The attached page is captioned "VERSION WITH MARKINGS TO SHOW CHANGES MADE."

Respectfully submitted,

YOUNG & THOMPSON

By _____
Roland E. Long, Jr.
Attorney for Applicant
Registration No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone: 521-2297

February 20, 2003

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS:

Claim 1 has been amended as follows:

--1. (amended) Method for protecting data communication traffic through a communication link between a first communication station (11) and a second communication station (12), in which the data is dispatched according to a data protocol from the second communication station to the first communication station, comprising the steps of:

(i) receiving the data from the second communication station (12) in a data communication protection device (10);

(ii) comparing the data protocol of the data with at least one [standardised] standardized protocol in the data communication protection device (10), [characterised] characterized by

(iii) providing the data communication protection device (10) in the communication link, the data from the second communication station (12) to the first communication station (11) passing through the data communication protection device (10); and

(iv) forwarding data of which the data protocol complies with the at least one [standardised] standardized protocol from the data communication protection device (10) to the first communication station (11), and not forwarding data of which the data protocol does not comply with the at least one

[standardised] <u>standardized</u> protocol from the data communication protection device to the first communication station <u>by physically interrupting the communication link between the first communication station (11) and the second communication station (12).</u>--

Claim 4 has been amended as follows:

--4. (amended) Data communication protection device (10) arranged for protecting data communication traffic between a first communication station (1) and a second communication station (12), data being dispatched according to a data protocol from the second communication station to the first communication station, the data communication protection device comprising memory means (14) for storing data characteristics of at least one [standardised] <u>standardized</u> protocol, the data communication protection device (10) further being arranged for comparing the data protocol of the data with the at least one [standardised] <u>standardized</u> protocol, [characterised] <u>characterized</u> in that the data communication protection device (10) further comprises

- a first link for linking the data communication protection device (10) to the first communication station (11), and a second link for linking the data communication protection device (10) to the second communication station (12), the data passing from the second communication station to the first communication station through the data communication protection device;

- comparison/forwarding means (15) for forwarding data received through the second link of which the data protocol complies with the at least one [standardised] <u>standardized</u> protocol from the data communication protection device (10) through the first link, and not forwarding data of which the data protocol does not comply with the at least one [standardised] <u>standardized</u> protocol from the data communication protection device (10) through the first link <u>by physically interrupting the</u> <u>communication link between the first communication station (11)</u> <u>and the second communication station (12)</u>.--